USAAC Acceptable Use Policy
For Unclassified Networks

1. Understanding. Provide understanding to all users that they have the primary responsibility to safeguard the information contained within the USAAC IAA (Integrated Automation Architecture) from unauthorized or inadvertent modification, disclosure, destruction, denial of service and to prevent unauthorized use.

2. Access. Access to this network is for official use and authorized purposes only as set forth in DOD Directive 5500.7-R, "Joint Ethics Regulation", Army Regulation 25-1 and 380-67, and USAAC policies.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. Classified information is strictly prohibited on USAAC IAA AISs (Automated Information Systems).

5. Unclassified information processing. USAAC IAA is the primary unclassified information system for the United States Army Accessions Command.

a. USAAC IAA provides unclassified communication to external DOD and other United States Government organizations. Primarily, this is done via electronic mail and Internet networking protocols, i.e., web, https and other work-related protocols.
b. USAAC IAA is approved to process UNCLASSIFIED, SENSITIVE information in accordance with DoD, Army and USAAC regulations.
c. USAAC IAA and the Internet, as viewed by the USAAC, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

6. Individual understanding and acceptance of minimum-security rules and requirements. As a USAAC IAA system user, I will follow the applicable minimum-security rules and requirements:

a. I understand that personnel are not permitted access to the USAAC IAA, unless in complete compliance with the USAAC personnel security requirement for operating Army AIS in a sensitive mission-critical environment.
b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification and non-standard threats such as social engineering) before receiving system access.
c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this

account. (I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.)

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware or public domain software.
e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment or compact disk.
f. I will not attempt to access or process data exceeding the authorized IS classification level.
g. I will not alter, change, configure or use operating systems or programs, except as specifically authorized.
h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.
i. I will safeguard and mark with the appropriate classification level all information created, copied, stored or disseminated from the IS and will not disseminate it to anyone without a specific need-to-know.
j. I will not utilize Army- or DOD-provided AISs for commercial financial gain or illegal activities.
k. I will not perform maintenance on any AIS for which I am responsible; however, I will allow maintenance to be performed by the System Administrator (SA).
l. I will use screen locks and logoff the workstation when not in use or when departing the area.
m. I will immediately report any suspicious output, files, shortcuts, or system problems to the USAAC SA, IASO or other IA staff and cease all activities on the system.
n. I will address any questions regarding policy, responsibilities, and duties to USAAC SA, IASO, or other IA staff.
o. I understand that each AIS is the property of the Army and is provided to me for official and authorized uses.
p. I understand that each AIS is subject to monitoring for security purposes and to ensure that use is authorized.
q. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.
r. I understand that monitoring of USAAC IAA will be conducted for various purposes (e.g., audit requirements, due diligence, to respond to a compelling event) and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.
s. I understand the following activities are samples which define unacceptable uses of an Army AIS:
   - unauthorized use of an AIS during duty hours
   - use of an AIS for involvement with gambling, profit-making, spam, sexual content, profanity.
   - access to unauthorized sites (e.g., pornography, streaming video & audio)
   - access to show unauthorized services (e.g., peer-to-peer, distributed computing)

- unauthorized use of e-mail use including but not limited to auto-forwarding to non-.mil accounts, sending mass-mailing, hoaxes.

t. I comprehend that policy violations may result in loss of access to USAAC AISs, criminal prosecution, administrative action and/or civil penalties.
u. I understand that the authority for soliciting my social security number (SSN) is Executive Order 9397. The information below will be used to identify me, and may be disclosed to law enforcement authorities for investigating or prosecuting violations.
v. I understand that disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to USAAC AISs.

7. Personal acknowledgement. I have read the above requirements regarding use of USAAC access systems. I understand my responsibilities regarding these systems and the information contained in them. I have had questions regarding acceptable use answered prior to signing.

Directorate/Division/Branch	Date
Last Name, First, MI	Rank/Grade
SSN	Phone Number
Signature	